Hasse Invariants and Anomalous Primes for Elliptic Curves with Complex Multiplication

by

Loren D. Olson *

The purpose of this article is to examine the Hasse invariants of certain elliptic curves defined over $\mathbb{Q}$ admitting complex multiplication. This was motivated by a desire to understand some of Mazur's results [7] on anomalous primes. In particular, we study curves of the form $Y^2 = X^3 + a_4X$ and $Y^2 = X^3 + a_6$ in detail. Deuring's formula for the Hasse invariant takes on a particularly simple form in these 2 cases. By combining this fact with some standard facts in the theory of complex multiplication, one can obtain information about the Hasse invariant. By considering special cases of these classes of curves, we obtain a number of results in elementary number theory concerning certain binomial coefficients. For all elliptic curves C defined over $\mathbb{Q}$ with field of complex multiplication $\mathbb{Q}(\sqrt{m})$, $m < 0$ and square-free, we show that the anomalous primes for C must be members of the quadratic progression $[(-mf^2)t^2 + 1]/4$ where f is the conductor of $\mathrm{End}(C)$ in the ring of integers in $\mathbb{Q}(\sqrt{m})$. As corollaries we obtain specific results for certain curves,

* The author was partially supported by NAVF (Norges almenvitenskapelige forskningsråd).

e.g. if $f = 2$, then C has no anomalous primes.

The first section of this paper establishes notation and underlying assumptions and collects together several well-known results and their consequences, which we shall use throughout the succeeding sections. Next we discuss the curves $Y^2 = X^3 + a_4X$, and in the third section we consider the curves $Y^2 = X^3 + a_6$. The final section is devoted to the general phenomenon of anomalous primes for elliptic curves admitting complex multiplication.

§ 1. Some classical results and their consequences.

Let C be an elliptic curve defined over $\mathbb{Q}$, i.e. a non-singular complete curve of genus 1 defined over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational point e. Any such curve has a Weierstrass model given by an affine equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

where $a_i \in \mathbb{Z}$. In projective space the curve is defined by

$$Y^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.2}$$

The unit element for the group law on C is the $\mathbb{Q}$-rational point $e = (0,1,0)$ and Z is a uniformizing parameter at e. If we expand the invariant differential $\omega = \frac{dX}{2Y+a_1X+a_3}$ in terms of Z, we obtain

$$\frac{\omega}{dZ} = C_0 + C_1Z + C_2Z^2 + \ldots\ldots \tag{1.3}$$

with $C_i \in \mathbb{Z}$.

Recall that if C has good reduction at a prime p, then the coefficient C_{p-1} of Z^{p-1} regarded modulo p is the Hasse invariant of C at p. Over any field of characteristic $\neq 2$ or 3,

one may assume that C is given by the affine equation

$$Y^2 = X^3 + a_4X + a_6 \tag{1.4}$$

i.e. that $a_1 = a_2 = a_3 = 0$. In this case, a classical result of Deuring [2] gives an explicit formula for the Hasse invariant of C in terms of a_4 and a_6.

Theorem 1.1 (Deuring). Let C be an elliptic curve defined over $\mathbb{Q}$ given by the affine equation $Y^2 = X^3 + a_4X + a_6$ with $a_4, a_6 \in \mathbb{Z}$. Let $p \geq 5$ be a prime where C has good reduction. Let $P = (\frac{1}{2})(p-1)$. Then the Hasse invariant of C at p is given by

$$C_{p-1} = \sum_{\substack{i\geq o, h\geq o \\ 2h+3i=P}} \frac{P!}{i!h!(P-h-i)!}\, a_4^h\, a_6^i \pmod{p} \tag{1.5}$$

A proof may be found either in Deuring [2] or Manin [6].

Let p be a prime where C has good reduction. Then the zeta-function of C over $\mathbb{Z}/p$ has the form

$$Z(t) = \frac{1-f_pt+pt^2}{(1-t)(1-pt)} \tag{1.6}$$

where f_p is the trace of the Frobenius F_p. $f_p = 1 + p - N_p$ where N_p is the number of points on C which are rational over $\mathbb{Z}/p$. The Riemann hypothesis for elliptic curves over finite fields says that the roots of $1 - f_pt + pt^2$ have absolute value $p^{\frac{1}{2}}$. This implies that

$$-2p^{\frac{1}{2}} < f_p < 2p^{\frac{1}{2}} \tag{1.7}$$

Given a prime p, let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol with respect to p. We can express f_p with the help of the Legendre

symbol as follows.

Theorem 1.2 Let C be an elliptic curve defined over $\mathbb{Q}$ given by the equation $Y^2 = X^3 + a_4X + a_6$ with $a_4, a_6 \in \mathbb{Z}$. Let p be a prime such that C has good reduction modulo p. Then

$$f_p = - \sum_{t \bmod p} \left(\frac{t^3+a_4t+a_6}{p}\right) \tag{1.8}$$

Among other things, Theorem 1.2 is extremely useful for computing examples.

The connection between f_p and the Hasse invariant is given by the following result.

Theorem 1.3 (Manin). Let C be an elliptic curve defined over $\mathbb{Q}$ and p a prime where C has good reduction. Then

$$C_{p-1} \equiv f_p \pmod{p} \tag{1.9},$$

i.e. the Hasse invariant C_{p-1} of C and the trace f_p of the Frobenius at p are congruent modulo p.

A proof may be found in either Manin [6] or Honda [4,5].

One of the important consequences of this is that, combined with the Riemann hypothesis, it allows one to read off the value of f_p and thus N_p from the value of the Hasse invariant for almost all primes p.

Corollary 1.4. Let C be an elliptic curve over $\mathbb{Q}$ and p a prime where C has good reduction.

(1) If $p \geq 3$, then $f_p = 0 \iff f_p \equiv 0 \pmod{p}$

(2) If $p \geq 7$, then $f_p = 1 \iff f_p \equiv 1 \pmod{p}$

(3) If $p \geq 17$, then f_p and N_p are uniquely determined by the Hasse invariant.

Proof: (1) If $p = 3$, then the Riemann hypothesis implies that $f_p = -3, 0,$ or $3,$ and so $N_p = 1, 4,$ or 7. C may be written in the form $Y^2 = X^3 + a_2X^2 + a_4X + a_6$. If $X^3 + a_2X^2 + a_4X + a_6$ has a zero in $\mathbb{Z}/3$, then $f_p \equiv 0 \pmod 3 \iff N_p = 4 \iff f_p = 0$. Assume $X^3 + a_2X^2 + a_4X + a_6$ has no zero in $\mathbb{Z}/3$. Then $f_p = -3 \iff X^3 + a_2X^2 + a_4X + a_6$ takes on the value 1 for all $x \in \mathbb{Z}/3$, and $f_p = 3 \iff X^3 + a_2X^2 + a_4X + a_6$ takes on the value -1 for all $x \in \mathbb{Z}/3$. In either case $X^3 + a_2X^2 + a_4X + a_6 = (X^3 - 1) + b$ where b is the value indicated and this polynomial always has a zero in $\mathbb{Z}/3$, a contradiction. Assume now that $p \geq 5$. $|f_p| < 2p^{\frac{1}{2}}$ by the Riemann hypothesis.
If $p \geq 5$, then $2p^{\frac{1}{2}} < p$, so $|f_p| < p$.
(2) If $p \geq 7$, then $-(p-1) < 2p^{\frac{1}{2}} < f_p < 2p^{\frac{1}{2}} < (p-1)$.
(3) If $p \geq 17$, then $2p^{\frac{1}{2}} < p/2$. Thus $-p/2 < -2p^{\frac{1}{2}} < f_p < 2p^{\frac{1}{2}} < p/2$, and so f_p (and hence also N_p) is uniquely determined by its residue class modulo p.

Remark. That part (2) does not hold for $p < 7$, is shown by considering $Y^2 = X^3 + 3X$ for $p = 5$ where $f_p = -4$. That part (3) does not hold for $p < 17$, may be seen by examining the two curves $Y^2 = X^3 + X$ and $Y^2 = X^3 + 7$ over $\mathbb{Z}/13$ which have $f_p = -6$ and $f_p = 7$ respectively.

Definition. Let C be an elliptic curve defined over $\mathbb{Q}$. A prime p is called anomalous for C if C has good reduction at p and $f_p \equiv 1 \pmod p$.

That such primes are of condiderable interest is indicated by Mazur's results [7]. Part (2) of Corollary 1.4 above is just part (iii) of Lemma 5.14 in Mazur [7].

§ 2. Curves of the form $Y^2 = X^3 + a_4X$

Throughout this section we assume that C is an elliptic curve defined over $\mathbb{Q}$ by $Y^2 = X^3 + a_4X$ with $a_4 \in \mathbb{Z}$. These curves admit complex multiplication by $i = \sqrt{-1}$. They have been studied at considerable length by Davenport and Hasse in [1].

Theorem 2.1. Assume C has good reduction at the prime p, $p \geq 5$.

(1) If $p \not\equiv 1 \pmod 4$, then $f_p = 0$ and $N_p = p+1$.

(2) If $p \equiv 1 \pmod 4$, then $f_p \equiv \binom{2n}{n} a_4^n \pmod p$ for $p = 4n+1$, and hence $f_p \not\equiv 0 \pmod p$.

(3) If $p \equiv 1 \pmod 4$ and $p > 5$, then $f_p \neq 1, -1$ and hence $f_p \not\equiv 1, -1 \pmod p$.

Proof: By Theorem 1.2, $f_p = -\sum_{t \bmod p} \left(\frac{t^3+a_4t}{p}\right) = -\left(\frac{0}{p}\right) - \sum_{0<t<p} \left(\frac{t^3+a_4t}{p}\right) = -\sum_{0<t\leq\frac{p-1}{2}} \left[\left(\frac{t^3+a_4t}{p}\right) + \left(\frac{-t^3-a_4t}{p}\right)\right] =$

$-\sum_{0<t\leq\frac{p-1}{2}} \left[\left(1+\left(\frac{-1}{p}\right)\right)\left(\frac{t^3+a_4t}{p}\right)\right] = \left(1+\left(\frac{-1}{p}\right)\right)\left[-\sum_{0<t\leq\frac{p-1}{2}} \left(\frac{t^3+a_4t}{p}\right)\right]$. Let

$S = -\sum_{0<t\leq\frac{p-1}{2}} \left(\frac{t^3+a_4t}{p}\right)$. Then $f_p = \left(1+\left(\frac{-1}{p}\right)\right)S$. If $p \not\equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and so $f_p = 0$, hence (1). Assume now that $p \equiv 1 \pmod 4$. By Deuring's formula and Manin's theorem, $f_p \equiv \binom{2n}{n} a_4^n \pmod p$. Since C has good reduction at p, $a_4 \not\equiv 0 \pmod p$. Thus $f_p \not\equiv 0 \pmod p$, and hence (2). If $p \equiv 1 \pmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $f_p = \left(1+\left(\frac{-1}{p}\right)\right)S = 2S$, so $f_p \neq 1, -1$. If $p > 5$, then $f_p \not\equiv 1, -1 \pmod p$ by Corollary 1.4, part (2).

Corollary 2.2. If $p \neq 5$, then p is not an anomalous prime for C. $p = 5$ is an anomalous prime for $C \iff a_4 \equiv 3 \pmod 5$.

Proof: If p is anomalous for C, then p must be 5 by Theorem 2.1. Using Theorem 1.2, we can check the four different non-zero residue classes modulo 5 and we obtain $a_4 \equiv 1 \Rightarrow f_p = 2$, $a_4 \equiv 2 \Rightarrow f_p = 4$, $a_4 = 3 \Rightarrow f_p = -4$, and $a_4 \equiv 4 \Rightarrow f_p = -2$.

A rather amusing result in elementary number theory is the following.

Corollary 2.3. Let $p \equiv 1 \pmod 4$ be a prime with $p = 4n+1$. Let $a \in \mathbb{Z}$ be such that $a \not\equiv 0 \pmod p$. Then $\binom{2n}{n}a^n \not\equiv 0,1,-1 \pmod p$, unless $p = 5$ and $a \equiv 3 \pmod 5$ (so that $\binom{2n}{n}a^n \equiv 1 \pmod p$) or $p = 5$ and $a \equiv 2 \pmod 5$ (so that $\binom{2n}{n}a^n \equiv -1 \pmod p$). In particular, $\binom{2n}{n} \not\equiv 0,1,-1 \pmod p$.

For $p = 4n+1$, we have seen that modulo p, f_p is given by $\binom{2n}{n}a_4^n$. The endomorphism $a \mapsto a^n$ of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ has n elements in its kernel (the roots of $X^n - 1$) and its image consists of 4 elements, namely the n-th power residues modulo p (the roots of $X^4 - 1$). Thus there are exactly 4 possibilities for the value of f_p modulo p, namely those corresponding to the 4 different n-th power residues multiplied by $\binom{2n}{n}$ modulo p. One also sees that $\binom{2n}{n}$ can never be a 4-th root of 1 modulo p for $p > 5$.

Proposition 2.4. Let $p = 4n+1$ be a prime. Then $\binom{2n}{n} \equiv 2 + 4s$ with $-2p^{\frac{1}{2}} < 2 + 4s < 2p^{\frac{1}{2}}$.

Proof: Consider the curve C given by $Y^2 = X^3 + X$. $f_p \equiv$

$\binom{2n}{n} \pmod p$. C has 4 points in the kernel of multiplication by 2 rational over $\mathbb{Z}/p\mathbb{Z}$. Thus $4 \mid N_p$. $f_p = 1 + p - N_p$ implies that $2 \mid f_p$ but $4 \nmid f_p$. Write $f_p = 2 + 4s$. By the Riemann hypothesis $-2p^{\frac{1}{2}} < 2 + 4s < 2p^{\frac{1}{2}}$.

The standard application of complex multiplication to the curve C proceeds as follows: Let $i = \sqrt{-1}$. i is a primitive 4-th root of 1 . The elliptic curve C admits complex multiplication by i , and the endomorphism ring of C is $\mathbb{Z}[i]$, the ring of integers in $\mathbb{Q}(i)$. If $p \equiv 1 \pmod 4$ and we have good reduction at p , then the Hasse invariant is non-zero at p by Theorem 2.1 and thus the endomorphism ring of C over $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}[i]$. If F_p denotes the Frobenius at p , then F_p is a root of the characteristic polynomial $X^2 - f_pX + p$ and $F_p \in \mathbb{Z}[i]$. We have $X^2 - f_pX + p = (X-F_p)(X-\bar{F}_p) = X^2 - (F_p+\bar{F}_p)X + F_p\bar{F}_p$ and so

$$p = F_p\bar{F}_p \tag{2.1}$$

and

$$f_p = F_p + \bar{F}_p \tag{2.2}$$

In the ring of Gaussian integers $\mathbb{Z}[i]$, one has a complete knowledge of the factorization of primes. $\mathbb{Z}[i]$ is principal, and the group of units is cyclic of order 4 consisting of $1,-1,i,-i$. Given a prime $p \equiv 1 \pmod 4$, p can be factored as $p = \pi\bar{\pi}$ with π and $\bar{\pi}$ irreducible in $\mathbb{Z}[i]$. They are uniquely determined up to a unit. Thus F_p can be written as either $i^r\pi$ or $i^r\bar{\pi}$ with $0 \le r \le 3$. If $F_p = i^r\pi$, then $\bar{F}_p = i^{4-r}\bar{\pi}$. There are only 4 possibilities for f_p , namely $\{i^r\pi + i^{4-r}\bar{\pi} \mid 0 \le r \le 3\}$ for a given choice of π . This agrees with our previous result that there are exactly 4 possibilities for f_p corresponding to the n-th power residue classes modulo p . Fix a primitive root

α modulo p, $p = 4n+1$. Let $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ be the modular character given by $\chi(\alpha^c) = \exp(2\pi ic/4)$ for $c \in \mathbb{Z}$. Write $a_4 \equiv \alpha^c \pmod{p}$ with $0 \leq c < p-1$. Then $\chi(a_4) = \chi(\alpha^c) = \exp(2\pi ic/4) = (\exp(2\pi i/4))^c = i^c$. If we normalize the choice of π such that $\binom{2n}{n} \equiv -\pi - \bar{\pi} \pmod{p}$, then $f_p = -i^c\pi - i^{4-c}\bar{\pi} = -\chi(a_4)\pi - \bar{\chi}(a_4)\bar{\pi}$. χ is just the 4-th power residue symbol. Our choice of π agrees with the usual one in the theory of power residue symbols, namely $\pi \equiv \bar{\pi} \equiv 1 \pmod{(2+2i)}$. As a corollary, we obtain the following classical result of Davenport and Hasse [1].

Corollary 2.5. (Davenport-Hasse). (1) If $p \equiv 3 \pmod 4$, then $N_p = p+1$.
(2) If $p \equiv 1 \pmod 4$, then $N_p = p+1+\chi(a_4)\pi+\bar{\chi}(a_4)\bar{\pi}$.

Example. Let $p = 13$, so $p = 4n+1$ for $n = 3$. Let C be defined by $Y^2 = X^3 + 2X$. Thus $a_4 = 2$. 2 is a primetive root modulo 13, so $\chi(a_4) = i$, $\bar{\chi}(a_4) = -i$. $\pi = 3+2i$ and $\bar{\pi} = 3-2i$ are the normalized choices of π and $\bar{\pi}$ such that $\pi \equiv \bar{\pi} \equiv 1 \pmod{2+2i}$. $\binom{2n}{n} \equiv \binom{6}{3} \equiv -6 \equiv -\pi - \bar{\pi}$. Corollary 2.4 implies that $N_p = p+1+\chi(a_4)\pi+\bar{\chi}(a_4)\bar{\pi} = 13+1+i(3+2i)+(-i)(3-2i) = 10$. Thus $f_p = 1+p-N_p = 4$. Theorem 2.1 yields $f_p \equiv \binom{2n}{n}a_4^n \equiv \binom{6}{3}2^3 \equiv 4$. We could also have computed f_p by means of Theorem 1.2.

§ 3. Curves of the form $Y^2 = X^3 + a_6$

Throughout this section we assume that C is an elliptic curve defined over $\mathbb{Q}$ given by $Y^2 = X^3 + a_6$ with $a_6 \in \mathbb{Z}$. Such

curves admit complex multiplication by a primitive 3-rd root of 1 . One reason for considering these curves is that they provide an interesting example of the phenomenon of anomalous primes.

Proposition 3.1. Assume C has good reduction at the prime p, $p \geq 5$.

(1) If $p \not\equiv 1 \pmod 6$, then $f_p = 0$ and $N_p = p+1$.

(2) If $p \equiv 1 \pmod 6$, then $f_p \neq 0$ and $f_p \not\equiv 0 \pmod p$.

(3) If $p \equiv 1 \pmod 6$, then $f_p \equiv \binom{3n}{n} a_6^n \pmod p$ where $p = 6n+1$.

Proof: 1) If $p \not\equiv 1 \pmod 6$, then $3 \nmid (p-1)$. The endomorphism $t \mapsto t^3$ of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ is an isomorphism and $t \mapsto t^3 + a_6$ is a bijection from $\mathbb{Z}/p\mathbb{Z}$ onto itself. Therefore $f_p = - \sum_{t \bmod p} \left(\frac{t^3+a_6}{p}\right) = - \sum_{t \bmod p} \left(\frac{t}{p}\right) = 0$. $N_p = p+1-f_p = p+1$.

2) If $p \equiv 1 \pmod 6$, then $3 \mid (p-1)$ and $t \mapsto t^3$ gives an endomorphism of $(\mathbb{Z}/p\mathbb{Z})^*$ with a kernel of order 3 and whose image is a subgroup of index 3 . Let S be a set of coset representatives for the kernel. We have

$$f_p = - \sum_{t \bmod p} \left(\frac{t^3+a_6}{p}\right) = - \left(\frac{a_6}{p}\right) - 3 \sum_{t \in S} \left(\frac{t^3+a_6}{p}\right) \qquad (3.1)$$

Since C is assumed to have good reduction at p , $a_6 \not\equiv 0 \pmod p$ and $\left(\frac{a_6}{p}\right) = \pm 1$. If $f_p = 0$, then (3.1) implies that $3 \mid \left(\frac{a_6}{p}\right)$, which is nonsense. Therefore $f_p \neq 0$. Corollary 1.4, part (1) implies that $f_p \not\equiv 0 \pmod p$.

3) By Deuring's formula and Manin's theorem, $f_p \equiv \binom{3n}{n} a_6^n \pmod p$.

Remark. In the proof of Proposition 3.1, we could have proved 2) more easily by using 3). However, we will later have use for formula (3.1) which we derived above.

Corollary 3.2. Assume C has good reduction at the prime p, $p \geq 5$.

1) If a_6 is a square or -3 times a square, then $f_p \neq 1$ and $f_p \not\equiv 1 \pmod{p}$, and C has no anomalous primes.

2) If a_6 is a cube, then $f_p \neq 1, -1$ and $f_p \not\equiv 1, -1 \pmod{p}$, and C has no anomalous primes.

Proof: If $p \not\equiv 1 \pmod{6}$, then $f_p = 0$ by Proposition 3.1, part 1). We may therefore assume $p \equiv 1 \pmod{6}$. By formula (3.1), we have $f_p = -(\frac{a_6}{p}) - 3 \sum_{t \in S} (\frac{t^3+a_6}{p})$. If a_6 is a square or -3 times a square, then $(\frac{a_6}{p}) = 1$ since $(\frac{-3}{p}) = 1$ if $p \equiv 1 \pmod{6}$, cf. Hardy and Wright [3, p.75]. Thus $f_p = -1 - 3 \sum_{t \in S} (\frac{t^3+a_6}{p})$ and $f_p \neq 1$. By Corollary 1.4, part (2), $f_p \not\equiv 1 \pmod{p}$ either. Thus (1) is proved. If a_6 is a cube, then $-a_6$ is a cube and there exists $t \in S$ such that $t^3 + a_6 = 0$. If $p = 6n+1$, S has $2n$ elements, so the sum $\sum_{t \in S} (\frac{t^3+a_6}{p})$ is a sum of $2n-1$ terms equal to either -1 or 1. The sum must therefore be an odd integer and hence not 0. $f_p = -(\frac{a_6}{p}) - 3 \sum_{t \in S} (\frac{t^3+a_6}{p})$ cannot be 1 or -1. By arguing as in Corollary 1.4, $f_p \not\equiv 1, -1 \pmod{p}$ either. Thus (2) is proved.

The preceding corollary shows that for purposes of finding anomalous primes, one should at least begin by assuming that a_6 is neither a square, -3 times a square, nor a cube. However, by looking at $Y^2 = X^3 + 1$, we obtain some results concerning elementary number theory.

Proposition 3.3. Let p be a prime such that $p \equiv 1 \pmod{6}$ with $p = 6n+1$.

(1) $\binom{3n}{n} \not\equiv 0, 1, -1 \pmod{p}$.

(2) $\binom{3n}{n} \equiv 2 + 6s \pmod{p}$ with $-2p^{\frac{1}{2}} < 2 + 6s < 2p^{\frac{1}{2}}$ and $s \in \mathbb{Z}$.

(3) In particular, (i) $-p < 2 + 6s < p$

(ii) $-(p^{\frac{1}{2}}+1)/3 < s < (p^{\frac{1}{2}}-1)/3$

(iii) $|s| < p^{\frac{1}{2}}/3 + 1/3$

(4) $2 | (n-s)$, i.e. n and s have the same parity.

Proof: Let $a_6 = 1$.

(1) Apply Proposition 3.1 and Corollary 3.2.

(2) As in the proof of part (2) of Corollary 3.2, we see that $\sum_{t \in S} \left(\frac{t^3+1}{p}\right)$ is an odd integer. Write it as $-2s-1$. Formula (3.1) implies that $f_p = -\left(\frac{1}{p}\right) - 3 \sum_{t \in S} \left(\frac{t^3+1}{p}\right) = -1 - 3(-2s-1) = 2 + 6s$. The Riemann hypothesis (1.7) gives $|f_p| < 2p^{\frac{1}{2}}$, i.e. (2).

(3) An easy consequence of (2).

(4) Since $6 | (p-1)$, the polynomial $t^6 - 1 = (t^3-1)(t^3+1)$ has 6 roots in $\mathbb{Z}/p\mathbb{Z}$. There are 3 roots for $t^3 + 1$, and this gives us three non-trivial points of order 2 on C over $\mathbb{Z}/p\mathbb{Z}$. Thus $4 | N_p$. $N_p = 1 + p - f_p = 1 + (6n+1) - (2+6s) = 6(n-s)$. Hence $4 | 6(n-s)$ and $2 | (n-s)$.

We are interested in studying anomalous primes, i.e. primes p where C has good reduction and where $f_p \equiv 1 \pmod{p}$. We have seen in Proposition 3.1 , that $p \equiv 1 \pmod{6}$ is a necessary condition. Write $p = 6n + 1$ and use the previous notation of this section. p is an anomalous prime for C $\iff$ $\binom{3n}{n} a_6^n \equiv 1 \pmod{p}$. Since both a_6^n and 1 are n-th power residues modulo p , $\binom{3n}{n}$ must also be an n-th power residue in order for p to anomalous for C . This is equivalent to requiring that

$\binom{3n}{n}^6 \equiv 1 \pmod{p}$, i.e. that $\binom{3n}{n}$ is a root of $X^6 - 1 \equiv 0 \pmod{p}$.

Example. It is not always true that $\binom{3n}{n}$ is an n-th power residue.

Let $n = 2$, $p = 13$. Then $\binom{3n}{n} = \binom{6}{2} = 15$, so $\binom{3n}{n} \equiv 2 \pmod{13}$ and $\binom{3n}{n}^6 \equiv 2^6 \equiv -1 \pmod{13}$.

We are therefore interested in determining when $\binom{3n}{n}$ is an n-th power residue, i.e. when $\binom{3n}{n}$ is a 6-th root of 1 modulo p. $X^6 - 1 = (X^3+1)(X^3-1) = (X+1)(X^2-X+1)(X-1)(X^2+X+1)$. We know that $\binom{3n}{n} \neq 1,-1 \pmod{p}$ from Proposition 3.3. The only possibilities for $\binom{3n}{n}$ to be a 6-th root of 1 are that $\binom{3n}{n}$ be a root of either $F_1(X) = X^2 - X + 1$ (i.e. a primitive 6-th root of 1) or $F_2(X) = X^2 + X + 1$ (i.e. a primitive 3-rd root of 1). Both cases can occur as the following examples show.

Examples. (1) Let $n = 12$, $p = 73$. Then $\binom{36}{12}$ satisfies the equation $F_2(X) \equiv 0 \pmod{p}$. One may check this by using Proposition 3.4 below with $s = 1$.

(2) Let $n = 1$, $p = 7$. Then $\binom{3n}{n} = \binom{3}{1} = 3$ satisfies the equation $F_1(X) \equiv 0 \pmod{p}$.

Proposition 3.4. Let $p = 6n + 1$ be a prime, $p \neq 7,13$. Write $\binom{3n}{n} \equiv 2 + 6s \pmod{p}$ with $-2p^{\frac{1}{2}} < 2 + 6s < 2p^{\frac{1}{2}}$ as in Proposition 3.3. Then the following conditions are equivalent:

(1) $\binom{3n}{n}$ satisfies $F_2(X) \equiv 0 \pmod{p}$

(2) $\binom{3n}{n}$ is a primitive 3-rd root of 1 modulo p

(3) $36s^2 + 30s + 7 \equiv 0 \pmod{p}$

(4) $p = 36s^2 + 30s + 7$.

Proof: (1) <==> (2) Clear.

(1) <==> (3) $\binom{3n}{n} \equiv 2+6s \pmod{p}$, so

$$F_2\left(\binom{3n}{n}\right) \equiv \binom{3n}{n}^2 + \binom{3n}{n} + 1 \equiv 0 \pmod{p}$$

$$\iff (2+6s)^2 + (2+6s) + 1 \equiv 0 \pmod{p}$$

$$\iff 36s^2 + 30s + 7 \equiv 0 \pmod{p}$$

(4) => (3) Clear.

(3) => (4) For all integer values of s , $36s^2 + 30s + 7$ is positive. If $36s^2 + 30s + 7 \equiv 0 \pmod{p}$, write $36s^2 + 30s + 7 = rp$ with r a positive integer. We have $36s^2 + 30s + 7 = rp = r(6n+1) = 6rn + r$. Computing modulo 6 , we obtain $r \equiv 1 \pmod{6}$. We claim that $r = 1$ and this will finish the proof. If $r \neq 1$, then $r \geq 7$ and $36s^2 + 30s + 7 \geq 7p$. Using the inequality $-(p^{\frac{1}{2}}+1)/3 < s < (p^{\frac{1}{2}}-1)/3$ from Proposition 3.3, part (3) (ii), we obtain $36s^2 + 30s + 7 < 36((p^{\frac{1}{2}}+1)/3)^2 + 30((p^{\frac{1}{2}}-1)/3) + 7 \leq 4(p^{\frac{1}{2}}+1)^2 + 10(p^{\frac{1}{2}}-1) + 7 \leq 4p + 18p^{\frac{1}{2}} + 1$. If $p > 37$, then $4p + 18p^{\frac{1}{2}} + 1 < 7p$, so that $36s^2 + 30s + 7 < 7p$. Thus $r = 1$ unless $p \leq 37$. Checking the cases for $p \leq 37$ with the help of Table I, we discover that only $p = 7$ and $p = 13$ need be excluded.

Remark. Note that we have not proved that if p is a member of the quadratic progression $36x^2 + 30x + 7$ (and $p \neq 7,13$), then $\binom{3n}{n}$ is a primitive 3-rd root of 1 .

We are however, much more interested in the case where $\binom{3n}{n}$ is a primitive 6-th root of 1 as the following proposition indicates.

Table I

n	p	$\binom{3n}{n}$	$\binom{3n}{n} \bmod p$	$\binom{3n}{n}^6 \bmod p$
1	7	3	- 4	1
2	13	15	2	- 1
3	19	84	8	1
5	31	3003	- 4	4
6	37	18564	- 10	1

Proposition 3.5. Let $p = 6n+1$ be an anomalous prime for the elliptic curve C given by $Y^2 = X^3 + a_6$. Then $\binom{3n}{n}$ must satisfy $F_1(X) \equiv 0 \pmod p$, i.e. $\binom{3n}{n}$ must be a primitive 6-th root of 1.

Proof: If p is an anomalous prime for C, then $\binom{3n}{n} a_6^n \equiv 1 \pmod p$. Raising both sides to the 6-th power, we see that $\binom{3n}{n}$ must be a 6-th root of 1. $\binom{3n}{n} \not\equiv 1, -1 \pmod p$ by Proposition 3.3, so $\binom{3n}{n}$ must satisfy either $F_1(X) \equiv 0 \pmod p$ or $F_2(X) \equiv 0 \pmod p$. If $\binom{3n}{n}$ satisfies $F_2(X) \equiv 0 \pmod p$, then $\binom{3n}{n}^3 \equiv 1 \pmod p$, so $a_6^{3n} \equiv 1 \pmod p$, i.e. a_6 is a quadratic residue modulo p. As in the proof of Corollary 3.2, $f_p = -\left(\frac{a_6}{p}\right) - 3 \sum_{t \in S} \left(\frac{t^3+a_6}{p}\right) = -1 - 3 \sum_{t \in S} \left(\frac{t^3+a_6}{p}\right)$, and so $f_p \neq 1$ and $f_p \not\equiv 1 \pmod p$. Thus $\binom{3n}{n}$ must satisfy $F_1(X) \not\equiv 0 \pmod p$.

Theorem 3.6. Let $p = 6n+1$ be a prime, Write $\binom{3n}{n} \equiv 2 + 6s \pmod p$ with $-2p^{\frac{1}{2}} < 2 + 6s < 2p^{\frac{1}{2}}$ as in Proposition 3.3. Then the following conditions are equivalent:

(1) $\binom{3n}{n}$ satisfies $F_1(X) \equiv 0 \pmod p$

(2) $\binom{3n}{n}$ is a primiteve 6-th root of 1 modulo p

(3) $12s^2 + 6s + 1 \equiv 0 \pmod p$

(4) $p = 12s^2 + 6s + 1$

Proof: (1) <==> (2) Clear.

(1) <==> (3) $\binom{3n}{n} \equiv 2 + 6s \pmod p$, so

$$F_1\left(\binom{3n}{n}\right) \equiv \binom{3n}{n}^2 - \binom{3n}{n} + 1 \equiv 0 \pmod p$$

<==> $(2+6s)^2 - (2+6s) + 1 \equiv 0 \pmod p$

$\Longleftrightarrow (2+6s)^2 - (2+6s) + 1 \equiv 0 \pmod{p}$

$\Longleftrightarrow 36s^2 + 18s + 3 \equiv 0 \pmod{p}$

$\Longleftrightarrow 12s^2 + 6s + 1 \equiv 0 \pmod{p}$

(4) $\Rightarrow$ (3) Clear.

(3) $\Rightarrow$ (4) For all integer values of s, $12s^2 + 6s + 1$ is positive. If $12s^2 + 6s + 1 \equiv 0 \pmod{p}$, write $12s^2 + 6s + 1 = rp$ with r a positive integer. We have $12s^2 + 6s + 1 = rp = r(6n+1) = 6rn + r$. Computing modulo 6, we obtain $r \equiv 1 \pmod{p}$. We claim that $r = 1$, and this will finish the proof. If $r \neq 1$, then $r \geq 7$ and $12s^2 + 6s + 1 \geq 7p$. Using Proposition 3.3, we obtain $12s^2 + 6s + 1 < 12((1/3)(p^{\frac{1}{2}}+1))^2 + 6((1/3)(p^{\frac{1}{2}}-1)) + 1$

$\leq (4/3)(p^{\frac{1}{2}}+1)^2 + 2(p^{\frac{1}{2}}-1) + 1$

$\leq (4/3)p + (14/3)p^{\frac{1}{2}} + 1/3$

$< 7p$.

Contradiction, so $r = 1$.

Remark. We have not yet shown that if p is a member of the quadratic progression $12x^2 + 6x + 1$, then $\binom{3n}{n}$ is a primitive 6-th root of 1. However, we will show that this is indeed the case in Theorem 3.10 below.

The only primes which can be anomalous for an elliptic curve C given by $Y^2 = X^3 + a_6$ are those of the form $p = 12s^2 + 6s + 1$. Mazur [7, p.187] showed that if p is an anomalous prime for the curve C, then a necessary condition is that p be of the form $(3h^2+1)/4$ with $h \in \mathbb{Z}$. We can easily determine the relationship between h and s.

Proposition 3.7. Let $p = 6n + 1 = 12s^2 + 6s + 1 = (3h^2+1)/4$. Then

(1) $n = 2s^2 + s$

(2) $h^2 = 8n + 1$

(3) $h^2 = 16s^2 + 8s + 1 = (4s+1)^2$

Proof: Elementary algebra.

Lemma 3.8. Let $p = 12s^2 + 6s + 1$ be a prime. The two solutions to $F_1(X) \equiv 0 \pmod{p}$ are $2 + 6s$ and $-6s - 1$; these are the 2 primitive 6-th roots of 1 modulo p.

Proof: Just substitute $2 + 6s$ and $-6s - 1$ in $F_1(X)$.

We shall now use the fact that an elliptic curve C given by $Y^2 = X^3 + a_6$ admits complex multiplication by a primitive 3-rd root of 1. This will provide us with a proof that a sufficient condition for $\binom{3n}{n}$ to be a primitive 6-th root of 1 is that p belongs to the quadratic progression $12s^2 + 6s + 1$. In addition, we can study such primes more closely to determine conditions on a_6 with respect to p in order that p be an anomalous prime for C. Let $\xi = (\frac{1}{2})(1+\sqrt{-3})$. ξ is a primitive 6-th root of 1. $\xi^2 = (\frac{1}{2})(-1+\sqrt{-3})$ is a primitive 3-rd root of 1. The field extensions $\mathbb{Q}(\xi)$, $\mathbb{Q}(\xi^2)$, and $\mathbb{Q}(\sqrt{-1})$ coincide. The ring of integers is $\mathbb{Z}[\xi^2] = \mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$. Assume now that C has good reduction at p with $p = 6n + 1$.
The Hasse invariant at p is non-zero by Proposition 3.1. The endomorphism ring of C over $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}[\xi]$. If F_p denotes the Frobenius at p, then F_p is a root of the characteristic polynomial $X^2 - f_p X + p$ and $F_p \in \mathbb{Z}[\xi]$. $X^2 - f_p X + p = (X - F_p)(X - \bar{F}_p)$ $= X^2 - (F_p + \bar{F}_p)X + F_p\bar{F}_p$.

We have

$$p = F_p \bar{F}_p \tag{3.2}$$

and

$$f_p = F_p + \bar{F}_p \tag{3.3}$$

Now $p \equiv 1 \pmod 6$ implies that p splits in $\mathbb{Z}[\xi]$. $\mathbb{Z}[\xi]$ is principal and the group of units is cyclic of order 6 consisting of the powers of ξ. Given a prime $p \equiv 1 \pmod 6$, p can be factored as $p = \pi\bar{\pi}$ with π and $\bar{\pi}$ irreducible in $\mathbb{Z}[\xi]$. They are uniquely determined up to a unit. Thus F_p can be written as either $\xi^r\pi$ or $\xi^r\bar{\pi}$ for $0 \leq r \leq 5$. There are exactly 6 possibilities for f_p, namely $\{\xi^r\pi + \xi^{6-r}\bar{\pi} \mid 0 \leq r < 6\}$. This agrees with the fact that $f_p \equiv \binom{3n}{n} a_6^n \pmod p$, and the 6 possibilities for f_p are determined by the 6 possible values of the n-th power residues modulo p. Fix a primitive root α modulo p. Let $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathbb{C}^*$ be the modular character given by $\chi(\alpha^c) = \exp(2\pi ic/6) = (\exp(2\pi i/6))^c = \xi^c$. Write $a_6 \equiv \alpha^c \pmod p$ with $0 \leq c < p-1$. Then $\chi(a_6) = \chi(\alpha^c) = \xi^c$ is just the 6-th power residue symbol. If we normalize the choice of π such that $\binom{3n}{n} \equiv -\pi - \bar{\pi} \pmod p$, then $f_p = -\chi(a_6)\pi - \bar{\chi}(a_6)\bar{\pi} = -\xi^c\pi - \xi^{6-c}\bar{\pi}$.

Theorem 3.9. Let C be an elliptic curve given by $Y^2 = X^3 + a_6$. Assume that C has good reduction at p.

(1) If $p \not\equiv 1 \pmod 6$, then $N_p = p + 1$.

(2) If $p \equiv 1 \pmod 6$, then $N_p = p + 1 + \chi(a_6)\pi + \bar{\chi}(a_6)\bar{\pi}$.

Example. Let $n = 2$, $p = 13$. Let C be given by $Y^2 = X^3 + 2$, so that $a_2 = 2$. 2 is a primitive root modulo 13, so $\chi(a_6) = \xi$,

$\bar{\chi}(a_6) = \xi^5$. $p = (1-4\xi)(-3+4\xi)$. $\pi = 1 - 4\xi$ and $\bar{\pi} = -3 + 4\xi$ are such that $\binom{3n}{n} \equiv 2 \equiv -\pi - \bar{\pi}$. Theorem 3.9 implies that $N_p = p + 1 + \chi(a_6)\pi + \bar{\chi}(a_6)\bar{\pi} = 13 + 1 + \xi(1+4\xi + \xi^5(-3+4\xi) = 19$. Thus $f_p = 1 + p - N_p = -5$. By Proposition 3.1, we should have $f_p \equiv \binom{3n}{n} a_6^n \equiv \binom{6}{2} 2^2 \equiv -5$. One may also obtain the same result by using Theorem 1.2.

We can now apply these results to the curve $Y^2 = X^3 + 1$.

Theorem 3.10. Let $p = 6n + 1$ be a prime. Then $\binom{3n}{n}$ is a primitive 6-th root of 1 modulo p <==> p is of the form $12s^2 + 6s + 1$ with $s \in \mathbb{Z}$. In this case $\binom{3n}{n} \equiv 2 + 6s \pmod{p}$.

Proof: (⇒) This implication has already been proved in Theorem 3.6.

(⇐) Assume $p = 12s^2 + 6s + 1$ for $s \in \mathbb{Z}$. We want a factorization of p in $\mathbb{Z}[\xi]$. Let $\pi = -(4s+1) + (2s)\xi$ and $\bar{\pi} = -(2s+1) - (2s)\xi$ $p = \pi\bar{\pi}$ and $\pi + \bar{\pi} = -6s - 2$. We can now compute the possible values for f_p by computing $\xi^r\pi + \xi^{6-r}\bar{\pi}$ for $0 \leq r < 6$. These values are listed in Table II. From Proposition 3.3, we know that $\binom{3n}{n} \equiv 2 + 6t$ with $t \in \mathbb{Z}$ and $-2p^{\frac{1}{2}} < 2 + 6t < 2p^{\frac{1}{2}}$. Since $\binom{3n}{n}$ modulo p gives the Hasse invariant for the curve $Y^2 = X^3 + 1$, $\binom{3n}{n}$ modulo p takes on one of the values for f_p given in Table II. The only possibility is $s = t$. Thus $\binom{3n}{n} \equiv 2 + 6s \pmod{p}$. By Lemma 3.8, this is a primitive 6-th root of 1 modulo p .

Corollary 3.11. Let C be an elliptic curve given by $Y^2 = X^3 + a_6$. Assume that C has good reduction at p . Then p is anomalous for C <==>

(1) there exists $s \in \mathbb{Z}$ such that $p = 12s^2 + 6s + 1$, and

Table II

r	$\xi^r \pi$	$\xi^{6-r} \bar{\pi}$	$f_p = \xi^r \pi + \xi^{6-r} \bar{\pi}$
0	$-(4s+1) + (2s)\xi$	$-(2s+1) - (2s)\xi$	$-6s - 2$
1	$-(2s) - (2s+1)\xi$	$-(4s+1) + (2s+1)\xi$	$-6s - 1$
2	$(2s+1) - (4s+1)\xi$	$-(2s) + (4s+1)\xi$	1
3	$(4s+1) - (2s)\xi$	$(2s+1) + (2s)\xi$	$6s + 2$
4	$(2s) + (2s+1)\xi$	$(4s+1) - (2s+1)\xi$	$6s + 1$
5	$-(2s+1) + (4s+1)\xi$	$(2s) - (4s+1)\xi$	-1

(2) $a_6^n \equiv -6s - 1 \pmod{p}$ with $n = 2s^2 + s$.

Proof: ($\Rightarrow$) Proposition 3.1 implies that $p \equiv 1 \pmod 6$. Write $p = 6n + 1$. Proposition 3.5 implies that $\binom{3n}{n}$ must be a primitive 6-th root of 1 modulo p . Theorem 3.10 gives the existence of $s \in \mathbb{Z}$ such that $p = 12s^2 + 6s + 1$ and that $\binom{3n}{n} \equiv 2 + 6s \pmod p$. If p is anomalous, then $f_p \equiv \binom{3n}{n} a_6^n \equiv 1 \pmod p \Rightarrow a_6^n \equiv \binom{3n}{n}^{-1} \equiv (2+6s)^{-1} \equiv -6s - 1 \pmod p$.
($\Leftarrow$) $f_p \equiv \binom{3n}{n} a_6^n \equiv (2+6s)(-6s-1) \equiv 1 \pmod p$.

Remark. Part (2) in Corollary 3.11 is equivalent to saying that $\chi(a_6) = \exp(2\pi i 5/6)$.

§ 4. Anomalous primes for curves with complex multiplication

Throughout this section we assume that C is an elliptic curve defined over $\mathbb{Q}$ which admits complex multiplication, i.e. its ring of endomorphisms is an order in the ring of integers in a quadratic imaginary extension of $\mathbb{Q}$. We shall prove four main results here, all dealing with anomalous primes for the curve C .

Let $\mathbb{Q}(\sqrt{m})$ with $m < 0$ and m square-free be the field of complex multiplication for C . Let A be its ring of integers. The endomorphism ring of C , End(C), is a subring of A of finite index and may be written as $R_f = \mathbb{Z} + fA$ for f a uniquely determined positive integer. f is called the conductor of End(C) in A . Let p be a prime where C has good reduction, and assume that the Hasse invariant at p is non-zero. If F_p is the Frobenius at p , then F_p is a root of the characteristic polynomial $X^2 - f_p X + p$ and $F_p \in R_f$. Thus

$X^2 - f_pX + p = (X-F_p)(X-\bar{F}_p) = X^2 - (F_p+\bar{F}_p)X + F_p\bar{F}_p$.

As usual we have

$$p = F_p\bar{F}_p \tag{4.1}$$

and

$$f_p = F_p + \bar{F}_p \tag{4.2}$$

This means first of all that p is split in the extension $\mathbb{Q}(\sqrt{m})$. Since C is defined over $\mathbb{Q}$, its j-invariant is an element of $\mathbb{Q}$ and R_f must have class number 1 . There are precisely 13 such R_f's (cf. Serre [9]). The group of units in $A(\sqrt{m})$ is finite and cyclic. Let r be its order; r is either 2, 4 or 6. The number of factorizations (4.1) is r , and so the number of possible values for f_p in (4.2) is r . In § 2, we considered in detail the case $j = 2^6 3^3$ for such curves are of the form $Y^2 = X^3 + a_4X$. In § 3, we considered $j = 0$ where $Y^2 = X^3 + a_6$.

Theorem 4.1. If $m \equiv 2$ or $3 \pmod 4$, then C has no anomalous primes with the following two exceptions:

(1) $p = 3$, $m = -2$, $f = 1$, and C is of the form $Y^2 = X(X^2-4DX+2D^2)$ with $D \equiv -1 \pmod 3$.

(2) $p = 5$, $m = -1$, $f = 1$, and C is of the form $Y^2 = X^3 + a_4X$ with $a_4 \equiv 3 \pmod 5$.

Proof: Since $m \equiv 2$ or $3 \pmod 4$, $A = \mathbb{Z}[\sqrt{m}] = \{s+t\sqrt{m} \mid s,t \in \mathbb{Z}\}$. Let $R_f = \mathbb{Z} + fA$ be the endomorphism ring of C . Let p be an anomalous prime for C . Write $p = \pi\bar{\pi}$ with $\pi = a + fr$, $a \in \mathbb{Z}$, $r \in A$. Let $r = s + t\sqrt{m}$. $\pi = a + fr = a + f(s+t\sqrt{m}) = (a+fs) + ft\sqrt{m}$ and $\bar{\pi} = (a+fs) - ft\sqrt{m}$. $p = \pi\bar{\pi} = (a+fs)^2 - f^2t^2m$. $f_p = \pi + \bar{\pi} =$

$= 2(a+fs)$. Thus $f_p \neq 1$. If $p \geq 7$, then $f_p \not\equiv 1 \pmod{p}$ by Corollary 1.4, and p is not anomalous. We may thus assume that $p < 7$. If $p = 2$, then $f_p \equiv 0 \pmod{p}$, so 2 is not anomalous. Assume $p = 3$, We have

$$3 = \pi\bar{\pi} = (a+fs)^2 - f^2t^2m \tag{4.3}$$

What are the possible values in (4.3) ? By the Riemann hypothesis, $-4 < -2p^{\frac{1}{2}} < f_p < 2p^{\frac{1}{2}} < 4$, so that $f_p = 2(a+fs)$ must be equal to -2 in order that $f_p \equiv 1 \pmod{p}$. Hence $a + fs = -1$. Thus (4.3) becomes $3 = (-1)^2 - f^2t^2m = 1 - f^2t^2m$ or $2 = -f^2t^2m$. This is possible only if $f = 1$, $m = -2$, $t^2 = 1$. So $t = \pm 1$ and $3 = (-1+\sqrt{-2})(-1-\sqrt{-2})$ is the only possible factorization. Curves with $f = 1$ and $m = -2$ can be put in the form $Y^2 = X(X^2-4DX+2D^2)$. (cf. Rajwade [8].) If 3 is to be anomalous, then $D \not\equiv 0 \pmod{3}$. Checking the 2 cases $D \equiv \pm 1 \pmod{3}$ and counting the number of points N_p in each case gives $D \equiv -1$ as a necessary and sufficient condition. Assume now that $p = 5$. We have

$$5 = \pi\bar{\pi} = (a+fs)^2 - f^2t^2m \tag{4.4}$$

What are the possible values in (4.4) ? By the Riemann hypothesis, $-5 < -2p^{\frac{1}{2}} < f_p < 2p^{\frac{1}{2}} < 5$, so that $f_p = 2(a+fs)$ must be equal to -4 in order that $f_p \equiv 1 \pmod{p}$. Hence $a + fs = -2$. Thus (4.4) becomes $5 = (-2)^2 - f^2t^2m = 4 - f^2t^2m$ or $1 = -f^2t^2m$. This implies that $f = 1$, $m = -1$ and $t^2 = 1$. $t = \pm 1$. The only possible factorization is $5 = (-2+\sqrt{-1})(-2-\sqrt{-1})$. The only curves with $f = 1$, $m = -1$ are those of the form $Y^2 = X^3 + a_4X$ which we studied in § 2. Corollary 2.2 shows that $p = 5$ is anomalous for such a curve $\Longleftrightarrow a_4 \equiv 3 \pmod{4}$.

Theorem 4.2. If $m \equiv 1 \pmod 4$ and f is the conductor of $\mathrm{End}(C)$ in A, then all the anomalous primes for C are members of the quadratic progression $[(-mf^2)t^2+1]/4$.

Proof: Since $m \equiv 1 \pmod 4$, 1 and $(\frac{1}{2})(1+\sqrt{m})$ form an integral basis for A, i.e. $A = \{s + (t/2)(1+\sqrt{m}) \mid s,t \in \mathbb{Z}\}$.
Let $R_f = \mathbb{Z} + fA$ be the endomorphism ring of C. Let p be an anomalous prime for C. Then $p = \pi\bar{\pi}$ with $\pi = a + fr$, $a \in \mathbb{Z}$, $r \in A$. Let $r = s + (t/2)(1+\sqrt{m})$. Then $\pi = a + fr = (a+fs+(ft/2)) + (ft/2)\sqrt{m}$ and $\bar{\pi} = (a+fs+(ft/2)) - (ft/2)\sqrt{m}$. We have

$$p = \pi\bar{\pi} = (a+fs+(ft/2))^2 - f^2t^2m/4 \tag{4.5}$$

and

$$f_p = 2a + 2fs + ft \tag{4.6}$$

If $f_p = 1$, then $a + fs + (ft/2) = 1/2$ and $p = 1/4 - f^2t^2m/4 = [(-mf^2)t^2+1]/4$. If p is anomalous and $p \geq 7$, then $f_p = 1$ by Corollary 1.4. We may assume that $p < 7$. If $p = 2$ is anomalous, then the Riemann hypothesis implies that either $f_p = 1$ or $f_p = -1$. In either case, $(a+fs+(ft/2))^2 = 1/4$ and $p = 1/4 - f^2t^2m/4$. If $p = 3$ is anomalous then either $f_p = 1$ or $f_p = -2$. The case $f_p = 1$ is O.K.
Suppose $f_p = -2$. Then $3 = p = 1 - (f^2t^2m/4)$, or $2 = -f^2t^2m/4$, or $8 = -f^2t^2m$. But $m \equiv 1 \pmod 4$ and $m < 0$ implies that this is impossible. If $p = 5$ is anomalous, then either $f_p = 1$ or $f_p = -4$. The case $f_p = 1$ is O.K. If $f_p = -4$, then $5 = p = 4 - (f^2t^2m)/4$, or $1 = -f^2t^2m/4$, or $4 = -f^2t^2m$. But $m \equiv 1 \pmod 4$ and $m < 0$ implies that this is impossible.

Corollary 4.3. If the conductor f of $\mathrm{End}(C)$ in A is even, then C has no anomalous primes.

Proof: If $m \equiv 2$ or $3 \pmod 4$, we need only consider the 2 exceptions in Theorem 4.1, and they both have conductor $f = 1$. If $m \equiv 1 \pmod 4$, then an anomalous prime p for C must be of the form $p = 1/4 - (f^2t^2m)/4$ according to Theorem 4.2. If f is even, write $f = 2f_1$ for some $f_1 \in \mathbb{Z}$. Then $p = 1/4 - (4f_1^2t^2m)/4 = 1/4 - f_1^2t^2m$, which is nonsense since p and $f_1^2t^2m$ are integers.

Corollary 4.4. If $m \equiv 1 \pmod 8$, then C has no anomalous primes with the following exception: $m = -7$, $p = 2$, and $f = 1$, and C must have good reduction at $p = 2$ and have a non-trivial point of order 2 over $\mathbb{Z}/2\mathbb{Z}$.

Proof: Let p be an anomalous prime for C. By Theorem 4.2, $p = 1/4 - (f^2t^2m/4)$.
Reasoning as in Corollary 4.3, we may assume both f and t odd. Assume p is odd with $p = 2p_1 + 1$. Write $f = 2f_1 + 1$, $t = 2t_1 + 1$, and $m = 8m_1 + 1$. $f^2 = 4(f_1^2+f_1) + 1$ and $t^2 = 4(t_1^2+t_1)+1$. $f_1^2 + f_1$ is always even, and so is $t_1^2 + t_1$. Thus $f^2 \equiv 1 \pmod 8$ and $t^2 \equiv 1 \pmod 8$. $4p \equiv 1 - f^2t^2m \pmod 8$, so $4 \equiv 4(2p_1+1) \equiv 1 - f^2t^2m \equiv 1 - 1 \equiv 0 \pmod 8$. This is a contradiction, so p must be equal to 2. Then we have $8 = 4p = 1 - f^2t^2m$ with $m \equiv 1 \pmod 8$, $m < 0$, f and t odd and non-zero. Thus $7 = -f^2t^2m$. The only possibility is $f = 1$, $m = -7$, $t^2 = 1$. $p = 2$ is anomalous if and only if C has good reduction at $p = 2$ and f_p is odd. Since $f_p = 1 + p - N_p$, f_p is odd if and only if N_p is even, i.e. if and only if C has a non-trivial point of order 2 over $\mathbb{Z}/2\mathbb{Z}$.

Bibliography

1) H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, Reine Angew. Math. 172 (1934), 151-182.

2) M. Deuring, Die Typen der Multiplikatorenringe elliptischer Functionenkörper, Abh. Math. Sem. Univ. Hamburg 14 (1941), 197-272.

3) G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers. Fourth Edition. Oxford University Press, London, England, 1960.

4) T. Honda, Formal Groups and zeta-functions, Osaka J. Math. 5 (1968), 199-213.

5) T. Honda, On the theory of commutative formal groups, J. Math. Soc. Japan 22 (1970), 213-246.

6) Ju.I. Manin, The Hasse-Witt Matrix of an Algebraic Curve (in Russian), Izv. Akad. Nauk SSSR Ser. Mat. 25 (1961), 153-172. (= Amer. Math. Soc. Transl. (2) (45), 245-264.)

7) Barry Mazur, Rational Points of Abelian Varieties with Values in Towers of Number Fields, Invent. Math. 18 (1972), 183-266.

8) A.R. Rajwade, Arithmetic on curves with complex multiplication by $\sqrt{-2}$, Proc. Cambridge Philos. Soc. 64 (1968), 659-672.

9) J.-P. Serre, Complex Multiplication, in J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Thompson Book Company, Washington, D.C., U.S.A., 1967.